COMPUTER SYSTEM CONNECTED TO A DATA COMMUNICATIONS NETWORK

[001] This is a Continuation of International Application PCT/DE01/04820, with an international filing date of December 20, 2001, which was published under PCT Article 21(2) in German, and the disclosure of which is incorporated into this application by reference.

FIELD OF AND BACKGROUND OF THE INVENTION

[002] The invention relates to a computer system that is connected to a data communications network, e.g., the Internet or an Intranet. Such computer systems, which are typically individual computers, e.g., PCs, are increasingly exposed to computer viruses and unauthorized access to internal data. As a rule, virus scanners can detect and eliminate only known computer viruses but not viruses that are completely new and that have entirely different structures than previously known viruses. In particular, in the case of computers in administrative offices, banks, insurance companies, and in industry (e.g., for operating and monitoring automation systems), which increasingly communicate with other computer systems, e.g., control centers, via public data communications networks, infection with computer viruses can cause enormous damage. For example, programs called Trojan horses can infiltrate the computer masquerading as a benign application, and can secretly spy out internal data and transmit this data to an external location.

OBJECTS OF THE INVENTION

[003] Thus, it is one object of the invention to obtain secure protection against computer viruses, unauthorized access to internal data, and data loss in case of infection with a virus.

SUMMARY OF THE INVENTION

[004] According to one formulation of the invention, this and other objects are attained by a computer system that can be connected to a data communications network., wherein the computer system has a first computer and an independent, redundant second computer. The two computers match themselves by comparing their work results. The receipt of data from the data communications network is limited to the first computer, and the transmission of data to the data communications network is limited to the second computer. At least the initial processing of the received data is limited to the first computer, and data received but not verified or not verifiable by the first computer is stored in the second computer only in locked, i.e., non-processable form.

[005] The computer system, according to one exemplary embodiment of the invention, is composed of two parallel computers, which have practically the same hardware structure and which are configured with the same software. The two computers work in parallel, alternately, or by sharing the work. However, they regularly match themselves by comparing their work results, e.g., by horizontal parity checks, by parallel balance, or by comparing predetermined data. For example, this matching can be triggered by the user; or the matching can be started automatically, e.g., at the end of a program; when files are closed; when data is input or output; or when a memory is accessed. The two computers exchange data or accept offered data

only if the work results supplied by the computers match. In the context of this matching, malfunctions or corrupted data can thus be detected based on different work results.

[006] To achieve the required security, receiving data from the data communications network and at least the initial processing of the received data is limited to the first computer, while transmitting data to the data communications network is limited to the second computer. This can be achieved by a hardware or software transmission block or reception block, respectively. Instead of the transmission block, it may also be provided, for example, that only received data can be stored in the first computer, so that it is impossible to transmit any data other than the received data. Within the context of the initial processing of the received data, which is limited to the first computer, the received data can be verified. Therein, the second computer can accept and store only verified data in unlocked, i.e., processable form. In the case of e-mail messages, verifiable data include, for example, the address of the sender, the "subject" text and other partial data that can be completely verified depending on the software product, e.g., text formats (but not macros). Preferably, the data are independently verified in both computers, and are stored in the second computer only after the results have been matched. Unverified or non-verifiable data received by the first computer are accepted by the second computer only in locked (encapsulated), i.e., non-processable form. This is also true for new data, which is generated by processing the received data in the first computer. Such locked data can neither be opened nor processed in the second computer but can only be added as an attachment, e.g., to an e-mail message being sent.

[007] This makes it possible to ensure that the second, redundant computer, which is prevented by hardware or software means from receiving data from the data

communications network, remains free from computer viruses. In addition, no computer viruses can be transmitted to the outside world when data is being sent. Nor can data be fetched or corrupted by so-called Trojan horses. If the first computer is infected with computer viruses because of data received from the data communications network, then this infection is immediately detected when the two computers are matched. In this case, the first computer can be restored to a virus-free state by copying the state of the second computer onto the first computer, without any data or previously performed work being lost.

[008] To exclude the possibility that internal data of the computer system contained in a central data memory are corrupted or deleted because of a virus infection of the first computer, which is capable of receiving data, only the second computer has direct access to the internal data. The first computer receives the internal data only upon request via the second computer.

[009] If the required computer capacity is relatively large, an independent redundant third computer may be provided, in which case the second and third computer match one another by comparing their work results. For example, in the case of an automation system, the third computer can assume the automation functions while the first and the second computer are responsible for communication via the data communications network.

BRIEF DESCRIPTION OF THE DRAWINGS

[010] The computer system will now be described with reference to an exemplary embodiment depicted in the single drawing.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[011] The exemplary computer system, which is depicted in the drawing as a functional block diagram, has a first computer 1, a second, redundant computer 2 and an optional third computer 3. The computers 1, 2 and 3 - with the exceptions described below - each have the same hardware structure and are configured with the same software. The computer 1 is connected to a data communications network 6 via a receiver driver 4 and is unable to transmit data. The redundant computer 2 is connected to the data communications network 6 via a transmitter driver 5 and is unable to receive data. The optional third computer 3 is provided in case increased computing capacity is required, e.g., for operating and monitoring automation systems. Except for the initial processing of received data, which is limited to the first computer 1, and the increased computer capacity to be provided by the third computer 3, all the computers 1, 2 and 3 execute the same functions. Any user inputs using, for example, a keyboard 7 or a mouse 8, are supplied in parallel to all three computers 1, 2 and 3.

[012] The work results or processing results of the two computers 1 and 2 are matched in a first memory or memory area 9 by, e.g., a horizontal parity check, parallel balance, etc. Other memories or memory areas 10 and 11 are used for exchanging data associated with the result matching of the two computers 1 and 2. Data are exchanged, or offered data are accepted, only if the work results or processing results of the two computers 1 and 2 match.

[013] Data received by the computer 1 from the data communications network 6, e.g., e-mail messages, are only selectively forwarded to the second computer 2 in the context of the data exchange (e.g., address of sender, "subject" text) and only to the extent that the data can be completely verified (e.g., text formats, but not macros).

This verification is performed independently in the two computers 1 and 2. The data are transmitted and stored in the respectively other computer only if the verification results match. Therein, the initial processing of received data is limited solely to the first computer 1. Non-verifiable received data and new data, which are generated by processing the non-verifiable data in the computer 1, are transmitted only in locked or sealed form to the second, redundant computer 2 in the context of the data exchange. The second, redundant computer 2 can neither open nor process the locked or sealed data. These data can only be added in their locked or sealed form as an attachment to other data being sent, e.g., an e-mail message being sent.

[014] If the first computer 1 is infected with computer viruses because of received data, this infection is detected during the regular matching of the two computers 1 and 2. Because of the above-described security mechanisms in the data exchange between the two computers 1 and 2, the computer viruses cannot spread from the first computer 1 to the second computer 2. By copying the state of the second computer 2 to the first computer 1, the first computer 1 can be restored to its virus-free state without any loss of data. Moreover, the above-described security mechanisms preclude unauthorized access to internal data of the computer system via the data communications network 6.

[015] As mentioned above, larger computer capacities, if needed, are accomplished, for instance, by the optional third computer 3. In this case, the first computer 1 and the second computer 2 are responsible for communication via the data communications network 6. The third computer 3 matches with the second computer 2 via memories or memory areas 12, 13 and 14. For security reasons, the first computer 1 has no access to a central data memory 15 having common data. The

common data can be read preferably only by the computer 3 and, if necessary, the computer 2, and are made available to the first computer 1, if required or requested.

[016] The above description of the preferred embodiments has been given by way of example. From the disclosure given, those skilled in the art will not only understand the present invention and its attendant advantages, but will also find apparent various changes and modifications to the structures and methods disclosed. It is sought, therefore, to cover all such changes and modifications as fall within the spirit and scope of the invention, as defined by the appended claims, and equivalents thereof.